



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,083	10/16/2000	Craig L. Ogg	40630/RRT/S850	2004

23363 7590 03/31/2003

CHRISTIE, PARKER & HALE, LLP
350 WEST COLORADO BOULEVARD
SUITE 500
PASADENA, CA 91105

EXAMINER

BACKER, FIRMIN

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 03/31/2003

7

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/690,083

Applicant(s)

OGG ET AL.

Examiner

Firmin Backer

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 October 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-120 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-120 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 October 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ 6) ☐ Other: _____

DETAILED ACTION

This is in response to a letter for patent filed on October 16th, 2000 in which claims 1-120 are presented for examination. Claims 1-120 are pending in the letter.

Double Patenting

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-71 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-70 of copending Application No. 09/688,456. Although the conflicting claims are not identical, they are not patentably distinct from each other because they both define inventions that are obvious variations of each other and achieving the same end result. Accordingly, it would have been obvious to those in possession of the inventive concept disclosed in claims 1-71 are already included in the inventive concept disclosed in claims 1-70 of copending application 09/688,456.

Art Unit: 3621

Furthermore, one of ordinary skill in the art at the time the invention was made would have realized the exclusion of "*a state machine for determining a state corresponding to one or more commands available to an authenticating user*" in claim 1, and the substitution of "*determining a state in a state machine for availability of one or more commands*" by "*including cryptographically protected data using a stored secret*" in claim 41 of the copending application 09/688,456 are obvious expedient since the remaining element are defined in the claims. In re Karlson, 136 USPQ 184 (CCPA 1963).

3. Claims 72-120 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-56 of copending Application No. 09/688,452. Although the conflicting claims are not identical, they are not patentably distinct from each other because they both define inventions that are obvious variations of each other and achieving the same end result. Accordingly, it would have been obvious to those in possession of the inventive concept disclosed in claims 57-68 are already included in the inventive concept disclosed in claims 1-56 of copending application 09/688,452. Furthermore, one of ordinary skill in the art at the time the invention was made would have realized the substitution of "*a computer executable code for authenticating one or more users and verifying that the authenticated user is authorized to assume a role*" by "*a state machine for determining a state corresponding to one or more commands available to an authenticating user*" in claims 1, 30 and claims 72, 104 respectively of the copending applications are obvious expedient since the remaining element are defined in the claims. In re Karlson, 136 USPQ 184 (CCPA 1963).

4. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-120 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leon (U.S. Patent No 6,424,954) in view of Whitehouse (U.S. Patent No. 6,005,945).

7. As per claim 1, Leon teaches a cryptographic device (*SMD, 110a, 110b comprise a cryptographic module*) for securing data on a computer network (*network 100a, 100b, fig 1A, 1B*) comprising a processor (*processor, 210*) programmed to authenticate (*authenticate*) a plurality of users (*users, 120, fig 1A, 1B*) on the computer network (*network 100a, 100b, fig 1A, 1B*) for secure processing of a value bearing item (*postal indicium, fig 9*) wherein the processor include a state machine for determine a state corresponding to availability of one or more commands (*see abstract, figs 5a-7, column 9 line 35-67*), a cryptographic engine (*cryptographic module*) for cryptographically protecting data, and an interface (*interface, 222, 236, fig 2A*) for

Art Unit: 3621

communicating with the computer network (*see column 4 line 21-55*). Leon fails to teach a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users. However, Whitehouse teaches a memory (*memory, 154*) for storing (*stores*) security device transaction data (*records*) for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users (*see fig 4, column 8 lines 30-67*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system.

8. As per claims 2-8, Leon teaches a cryptographic device wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state (*see abstract, figs 5a-7, column 9 line 59-67*).

9. As per claim 9, Leon teaches a cryptographic device wherein on or more command corresponding to the uninitialized state includes a command for start initializing (*figs 6a-6e, column 10 lines 10-16*).

Art Unit: 3621

10. As per claim 10, Leon teaches a cryptographic device wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands (*see abstract, figs 5a –7, column 10 lines 10-16, 13 lines 26-47*).

11. As per claim 11, Leon teaches a cryptographic device wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support (*see column 11 lines 36-43*).

12. As per claim 12, Leon teaches a cryptographic device wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command (*see fig 5b, column 13 lines 63-14 line 31*).

13. As per claim 13, Leon teaches the inventive concept as disclosed in claims 1 and 11. Leon fail to teach a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command. However, Whitehouse teaches a cryptographic device wherein the commands for

Art Unit: 3621

session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command (*see column 9 lines 32-67*). Therefore, it would have been obvious to one of ordinary skill in that art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command because this would have avoided the need for key encryption in the user's computer.

14. As per claim 14, Leon teaches a cryptographic device wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands (*see column 13 lines 36-62*).

15. As per claim 15, Leon teaches a cryptographic device wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5*).

Art Unit: 3621

16. As per claim 16, Leon teaches a cryptographic device wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command (*see abstract, figs 5a-7, see column 9 line 35-67*).

17. As per claim 17, Leon teaches a cryptographic device wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command (*see column 8 line 63-9 line 19*).

18. As per claim 18, Leon teaches a cryptographic device wherein the one or more commands corresponding to the importing shares state include command for one more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command (*see column 8 line 63-9 line 19*).

19. As per claim 19, Leon teaches a cryptographic device wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command (*see column 10 lines 39-46*).

20. As per claim 20, Leon teaches a cryptographic device further comprising computer executable code to keep track of a present operational state (*see abstract, figs 5a-7, see column 9 line 35-67*).

21. As per claim 21, Leon teaches a cryptographic device wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation (*see fig 5A, column 12 lines 30-42, table 1 in column 12*).

22. As per claim 22, Leon teaches a cryptographic device wherein the cryptographic device includes a computer executable code for preventing unauthorized disclosure of data (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42*).

23. As per claim 23, Leon teaches a cryptographic device wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user (*see fig 1A, 1B*).

24. As per claims 24-27, Leon teaches a cryptographic device wherein the value bearing item include a postage value including a postal indicium comprises a digital signature, a

Art Unit: 3621

postage amount, an ascending register of used postage and descending register of available postage (*see fig 8F, table 3 column 42*).

25. As per claim 28-33, Leon teaches a cryptographic device wherein the value bearing item is a ticket, a bar code, a coupon, a currency, a traveler's check, a voucher (*see fig 9*).

26. As per claim 34, Leon teaches a cryptographic device wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list (*see fig 8F, table 3 column 42*).

27. As per claim 35, Leon teaches a cryptographic device wherein each security device transaction data includes information to define the present operational state of the device (*see abstract, figs 5a –7, see column 9 line 35-67*)

28. As per claim 36, Leon teaches a cryptographic device wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices (*see column 13 lines 48-62*).

Art Unit: 3621

29. As per claim 37-40, Leon teaches a cryptographic device wherein the processor and the cryptographic engine generate a master key set (MKS) including a Master Encryption Key (MEK) used to encrypt keys when stored outside the device and a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device exported to other cryptographic devices by any cryptographic device and wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 13 lines 48-62*).

30. As per claim 41, Leon teaches a cryptographic device wherein at least one of the plurality of users is an enterprise account (*see fig 1*).

31. As per claims 42 and 44, Leon teaches a method for securing (*SMD, 110a, 110b comprise a cryptographic module*) data (*postal/metering information*) on a computer network (*network 100a, 100b, fig 1A, 1B*) including a plurality of users (*users, 120, fig 1A, 1B*) comprising authenticating (*authenticate*) and authorizing (*authorizing*) the plurality of users (*users, 120, fig 1A, 1B*) for secure processing of a value bearing item (*postal indicium, fig 9*) and determining a state machine for availability of one or more commands (*see abstract, figs 5a-7, column 9 line 35-67*). Leon fails to teach a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users. However, Whitehouse teaches a memory (*memory, 154*) for storing (*stores*) security device transaction data (*records*) for ensuring authenticity and

Art Unit: 3621

authorization users, wherein the security device transaction data is related to the one of the plurality of users (*see fig 4, column 8 lines 30-67*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system.

32. As per claim 43, Leon teaches a method for securing of printing the value bearing item (*see fig 9*).

33. As per claim 45, Leon teaches a method for securing of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item (*see column 9 lines 1-10*).

34. As per claim 46, Leon teaches a method for securing of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation (*see column 8 line 45-61*).

35. As per claims 47-53, Leon teaches a method wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an

Art Unit: 3621

exporting shares state, an importing shares state, and an error state (*see abstract, figs 5a-7, see column 9 line 35-67*).

36. As per claim 54, Leon teaches a method wherein on or more command corresponding to the uninitialized state includes a command for start initializing (*see figs 5A, 5B, 6*).

37. As per claim 55, Leon teaches a method wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands (*see fig 5A, 5B, column 10 line 10-16*).

38. As per claim 56, Leon teaches a method wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5*).

39. As per claim 57, Leon teaches a method wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access

Art Unit: 3621

control database command, change password command, set clock command, and set Status command (*see column 8 line 45-62*).

40. As per claim 58, Leon teaches the inventive concept as disclosed in claims 1 and 11.

Leon fails to teach a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command. However, Whitehouse teaches a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command (*see column 9 lines 32-67*). Therefore, it would have been obvious to one of ordinary skill in that art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command because this would have avoided the need for key encryption in the user's computer.

41. As per claim 59, Leon teaches a method wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC,

Art Unit: 3621

and encryption and MAC translation commands (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42*).

42. As per claim 60, Leon teaches a method wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5*).

43. As per claim 61, Leon teaches a method wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command (*see column 8 lines 63-9 line 33*).

44. As per claim 62, Leon teaches a method wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command (*see fig 5A, column 12 lines 30-42, table 1 in column 12*).

Art Unit: 3621

45. As per claim 63, Leon teaches a method wherein the one or more commands corresponding to the importing shares state include command for one more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command (*see fig 5A, column 12 lines 30-42, table 1 in column 12*).

46. As per claim 64, Leon teaches a method wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command (*see column 10 lines 39-46*).

47. As per claims 65-68, Leon teaches a method of printing a postage value including a postal indicium comprises a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see fig 8F, table 3 column 42*).

48. As per claim 69-71, Leon teaches a method or printing a ticket, a bar code, a coupon, (*see fig 9*).

49. As per claim 72, Leon teaches a security system (*SMD, 110a, 110b comprise a cryptographic module*) for securing data (*postal/metering information*) in a computer network (*network 100a, 100b, fig 1A, 1B*) comprising a plurality of user terminals (*users, 120, fig 1A, 1B*) coupled (*connected*) to the computer network (*network 100a, 100b, fig 1A, 1B*), a cryptographic

Art Unit: 3621

device (*cryptographic key*) remote from the plurality of user terminals and coupled to the computer network, wherein the cryptographic device (*SMD, 110a, 110b comprise a cryptographic module*) includes a state machine (*state diagram/method, fig 6A*) for determining a state machine for availability of one or more commands available to authenticating user. Leon fails to teach a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user. However, Whitehouse teaches a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user (*see fig 3, 4 and 7, column 8 line 30-9 line 63*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data is related to a user because this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system.

50. As per claim 73, Leon teaches a security system wherein the security device transaction data related to a user is loaded into the cryptographic device when the user requests to operate on a value bearing item (*see fig 9*).

51. As per claims 74-80, Leon teaches a method wherein the state machine includes one or more of an uninitialized state, an initialized state, an operational state, an administrative state, an

Art Unit: 3621

exporting shares state, an importing shares state, and an error state (*see abstract, figs 5a-7, see column 9 line 35-67*).

52. As per claim 81, Leon teaches a method wherein on or more command corresponding to the uninitialized state includes a command for start initializing (*see figs 5A, 5B, 6*).

53. As per claim 82, Leon teaches a method wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands (*see fig 5A, 5B, column 10 line 10-16*).

54. As per claim 83, Leon teaches a method wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5*).

55. As per claim 84, Leon teaches a method wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access

Art Unit: 3621

control database command, change password command, set clock command, and set Status command (*see column 8 line 45-62*).

56. As per claim 85, Leon teaches the inventive concept as disclosed in claims 1 and 11. Leon fails to teach a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command. However, Whitehouse teaches a cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command (*see column 9 lines 32-67*). Therefore, it would have been obvious to one of ordinary skill in that art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's cryptographic device wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session, MAC command, session encrypt command, and session decrypt command because this would have avoided the need for key encryption in the user's computer.

57. As per claim 86, Leon teaches a method wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC,

Art Unit: 3621

and encryption and MAC translation commands (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42*).

58. As per claim 87, Leon teaches a method wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command (*see column 8 line 45-62*).

59. As per claim 88, Leon teaches a method wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42*).

60. As per claim 89, Leon teaches a method wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command (*see fig 5A, column 12 lines 30-42, table 1 in column 12*).

61. As per claim 90, Leon teaches a method wherein the one or more commands corresponding to the importing shares state include command for one more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command (*see fig 5E-5E-2, column 17 lines 47-54, 19 lines 33-42*).

62. As per claim 91, Leon teaches a method wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command (*see abstract, figs 5f, see column 18 line 18-40, 24 line 60-25 line 5*).

63. As per claim 92, Leon teaches a security system comprising computer executable code to keep track of a present operational state (*see column 8 line 45-62*).

64. As per claim 93, Leon teaches a security system wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation (*see column 8 line 45-62*).

65. As per claim 94, Leon teaches a security system wherein the system includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user (*see fig 1A, 1B*).

66. As per claims 95-98, Leon teaches a secured system wherein a postage value including a postal indicium comprises a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see fig 8F, table 3 column 42*).

67. As per claim 99-100, Leon teaches a security system wherein the value bearing item include a bar code is a ticket (*see fig 9*).

68. As per claim 101, Leon teaches a security system wherein each security device transaction data includes information to define the present operational state of the device (*see fig 6A, column 9 line 35-67*).

69. As per claim 102, Leon teaches a security system wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 11 lines 51-12 line 4, 13 line 47-62*).

70. As per claim 103, Leon teaches a method or printing a ticket, a bar code, a coupon, (*see fig 9*).

71. As per claim 104, Leon teaches a method for securing data (*SMD, 110a, 110b comprise a cryptographic module*) in a computer network (*network 100a, 100b, fig 1A, 1B*) having a

Art Unit: 3621

plurality of user terminals (*users, 120, fig 1A, 1B*) the method comprising and verifying that a user is authorized to assume a role and determining a state in a state machine for availability of one or more commands (*see fig 1A, 1B, 5A, 6A, column 9 lines 34-67*). Leon fail to teach an inventive concept of storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals storing a plurality of security device transaction data wherein each transaction data is related to one of the plurality of users. However Whitehouse teaches an inventive concept of storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals storing a plurality of security device transaction data wherein each transaction data is related to one of the plurality of users (*see fig 4, column 8 lines 30-9 line 31*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Leon's inventive concept to include Whitehouse's an inventive concept of storing information about a plurality of users using the plurality of terminals in a database remote from the plurality of securing the information about the users in the database by one or more of cryptographic devices remote from the plurality of user terminals storing a plurality of security device transaction data wherein each transaction data is related to one of the plurality of users this would have protected the privacy of those transaction and the privacy of the user thereby making easier for the system to retrieve and identify the user of the system.

Art Unit: 3621

72. As per claim 105, Leon teaches a method of printing the value bearing item (*see fig 9*).

73. As per claim 106, Leon teaches a method of loading a security device transaction data related to a user into one of the one or more of cryptographic devices when the user requests to operate on a value bearing item (*see column 9 lines 28-33, 13 lines 48-62, 15 lines 23-32*).

74. As per claim 107, Leon teaches a method of loading a security device transaction data related to the cryptographic device when the user requests to operate on a value bearing item (*see column 9 lines 28-33, 13 lines 48-62, 15 lines 23-32*).

75. As per claim 108, Leon teaches a method of authenticating the identity of each user and verifying that the identified user is authorized to assume a role and to perform a corresponding operation (*see column 8 lines 45-9 line 10*).

76. As per claims 109-115, Leon teaches a method of determining an uninitialized state, an initialized state, an operational state, an administrative state, an exporting shares state, an importing shares state, and an error state (*see fib 5A, 6A, column 9 lines 45-67*).

77. As per claims 116-120, Leon teaches a method of printing a postage value including a postal indicium comprises a digital signature, a postage amount, or a ticket (*see fig 9*).

Conclusion

78. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. *Cordey et al (U.S. Patent No. 6,466,921) teach a virtual postage metering system provides central management of all postage without the need to manage physical meters or PSDs*

b. *Amanda (U.S. Patent No 6,385,731)) teaches on-line electronic postage metering system that operates in conjunction with the United States Postal Service (USPS) that allows a user to print a postal indicium at home, at office, or any other desired place in a secure and fraud-free manner. A user computer and a user printer, electronically connected to the PSD server and the USPS computer, constitute an on-line electronic postage meter.*

c. *Kara et al (U.S. Patent No. 6,249,777) teach a demand program that may be coupled to a word processing program, or other process, residing within the first PC, thus allowing the user to request and subsequently print the postage indicia on correspondence or postal items generated by the coupled process.*

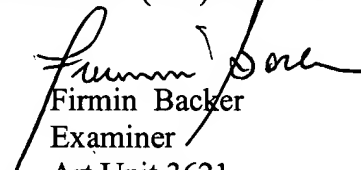
Art Unit: 3621

d. *Leon (U.S. Patent No. 6,381,589) teaches a secure processing unit interfaces with the local computer and performs the secure processing normally associated with a secure postal environment.*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.


Firmin Backer
Examiner
Art Unit 3621

March 13, 2003